MILWAUKEE POLICE DEPARTMENT

STANDARD OPERATING PROCEDURE

680 – COMPUTER EQUIPMENT, APPLICATIONS and SYSTEMS

GENERAL ORDER: 2012 - 03	**ISSUED**: February 7, 2012	**EFFECTIVE**: February 10, 2012
ACTION: Amends General Order 2010 – 30 (November 4, 2010)		

680.00 PURPOSE

This standard operating procedure is intended to provide guidelines for the use of computer equipment within the Department and to set guidelines for the use of various applications. This includes personally owned computers that are used in Department activities.

680.05 COMPUTER GUIDELINES

A. Computer resources are provided for Department business only. Personal and non-Department uses are prohibited.

B. Only software purchased, developed or otherwise obtained by the Department is to be used on Department equipment.

C. No additional computer hardware and/or computer peripheral equipment shall be installed, moved, removed, or reallocated without the written approval of the Information Technology Division. All hardware and peripheral equipment installations, moves, removals or re-allocations are the responsibility of the Information Technology Division.

D. Additional computer hardware, software applications and/or processes for new Departmental projects shall not be acquired through City Purchasing, Asset Forfeiture, grants, donations, etc. without first notifying the Information Technology Division for planning and scheduling. It is the responsibility of the Information Technology Division to ensure that additional computer hardware, software applications and/or processes are compatible and/or compliant with current MPD policies, DPW MOU infrastructure, City network policies, State CIB and Federal CJIS Security guidelines.

E. Computers and all associated peripherals, software, documentation and data, including instruction manuals, are not to be moved from their authorized location without the prior consent of the Information Technology Division.

F. Any program or work product developed on Department equipment or on Department time is the property of the City of Milwaukee and shall not be sold or given away without proper authorization.

G. In accordance with the purchase of hardware and software by the City of Milwaukee, the City is subject to the provisions of the copyright laws. As a practical matter, these laws prohibit the copying of computer software for other than archival and backup purposes.

H. In compliance with City of Milwaukee computer policy, the Information Technology Division will only support software meeting their software standards. Other authorized software running on Department computers must have the master disks, manuals and registration information next to the computer. If registration information cannot be supplied, the software must be removed immediately.

I. If shareware or public domain software is operating on a Department system, the documentation requirements established above must be maintained. In addition, a *Department Memorandum* (PM-9E) shall be submitted to the Information Technology Division for purposes of identifying ownership.

J. Periodic audits and preventative maintenance programs will be performed by the Information Technology Division. These procedures will ensure that only authorized software is operating on all Department systems and that the equipment is operating effectively and efficiently according to the purpose for which the equipment was acquired.

680.10 TIME AND eTIME SYSTEMS

The Transaction Information for the Management of Enforcement (TIME) System and eTIME (the web based application of the TIME system) provides a central system for the collection and dissemination of information of mutual concern to law enforcement agencies. It is an efficient and expeditious means by which the procurement, exchange and transmission of information with law enforcement agencies state and nationwide is accomplished. The system also provides an effective method of administrative communication for law enforcement purposes. The TIME and eTIME systems are interfaced with numerous local, state and national agencies, departments and files. It is of vital importance that regulations pertaining to its use be complied with to ensure individual rights are not violated and to minimize issues of liability. Data service agencies have agreed to make information available to law enforcement and criminal justice over the TIME, eTIME and NCIC Systems for the specific purpose of facilitating the administration of criminal justice. Any misuse of this information or violations of these understandings jeopardizes the availability of information for all participating agencies. The systems and the information contained therein must be protected from possible physical, natural and hardware vulnerabilities.

A. TIME Agency Coordinator

The TIME Agency Coordinator (TAC) is responsible for coordinating training of the functions of the terminal, ensuring compliance with NCIC and Crime Information Bureau (CIB) policy and regulations including validation and other requirements, and formatting training in conjunction with CIB certification, re-certification and specialized training classes. The TAC will ensure a proper number of Training Resources Available on the InterNet (TRAIN) Administrators are assigned to work locations/shifts that utilize the TIME system. The TAC will attend CIB TIME System TAC training within one year of appointment as the Department's TAC.

B. TRAIN Administrators

Each work location which utilizes the TIME system will be assigned at least one TRAIN Administrator. The TRAIN Administrators will assist the TAC to ensure all members at the work location requiring TIME certification are properly trained and re-certified.

C. Certification of TIME and eTIME System Users

1. Only those members who obtain and maintain the required Department of Justice (DOJ) training will be granted access to the TIME and eTIME systems. Members using the TIME and eTIME system may only use the system for purposes for which they were certified.

2. All members of the department who use Criminal Justice Information Systems (CJIS) or who routinely review criminal justice data as a position responsibility will be required to be re-certified every two (2) years. Re-certification notifications and administration will be handled by the Department's TAC.

D. Data Protection and Security

Data security is of the utmost concern and to ensure the security of sensitive law enforcement data the following guidelines will be employed:

1. [redacted]
REDACTED
requirement.

2. Background re-investigations (consisting of criminal history updates in addition to routine driver's license audits) will be conducted minimally every 5 years on all Department members who have access to Criminal Justice Information Systems.

3. Each member of the department having TIME and/or eTIME system privileges has been issued a unique system login. Members are required to log out or lock all Criminal Information Systems from unauthorized access when the member is not present at the system.

4. All transactions from criminal justice data systems are considered confidential and may not be released to non-law enforcement agencies or personnel.

5. Any individual authorized to use the TIME or eTIME System who receives a request for criminal justice information from another individual must ensure the person requesting the information is authorized to receive the data. Each data service has its own rules for secondary dissemination of records, which may include requirements for logging, identification of the purpose of the request and identification of the specific individual receiving the record. Most records may be legitimately disseminated to another criminal justice employee/agency when the purpose of the request is criminal justice related.

6. The printing and/or copying of criminal justice data will be limited to the time of need and reproductions limited to the smallest quantity to complete the job.

7. Printed criminal justice data will be securely disposed of when no longer needed. Printed media will be destroyed by shredding or by placing the media in secure shredding containers for later shredding.

E. Physical Security of Sensitive Law Enforcement Information

1. Any device (i.e. computer monitors, smart phone displays, etc.) that displays criminal justice information will be positioned in such a way as to prevent unauthorized individuals from accessing or viewing the criminal justice information.

2. Non-department members accessing any non-public area of a police facility that conducts Criminal Justice Information System transactions must sign-in on Form PL-7E *MPD Police Facility Visitor Log* prior to admittance into an area not normally designated as publicly accessible. See SOP 780 *Police Facilities Security* for full information on visitors to police facilities.

680.15 USE OF PERSONALLY-OWNED COMPUTERS

A. WRITTEN REQUEST

Members wishing to use personally owned computers for Department business shall submit their request on a Form PI-4 to their commanding officer. This report shall describe the functions to be performed by the computer and the objectives to be achieved.

B. SPECIAL PERMISSION

Personally owned computers shall not be connected to any Department telephone system or Department network without the specific permission of the Information Technology Division.

C. COMMANDING OFFICER'S RESPONSIBILITY

1. Approve or deny requests by members to use personally owned computers for Department business. This may be done only in cases where the computer is not connected to a Department telephone or network system.

2. When connection to a Department telephone or network system is required, the original request shall be forwarded to the Information Technology Division for review.

3. Copies of all requests, whether approved or denied, shall be maintained at the work location.

680.20 MEMBER'S RESPONSIBILITIES

A. Department members shall comply with the provisions of Milwaukee Police Department Rules and Procedures regarding the confidentiality of Department records, reports and information.

B. Computer input and output data shall be in compliance with the State of Wisconsin Open Records Laws.

C. Additional care shall be exercised concerning sensitive Department data. Sensitive data is defined as data that is not routinely available to the public. Under no circumstances is this information to be created, stored, processed or duplicated by members outside of official Department facilities without specific **written** permission of the member's commanding officer.

680.25 COMMANDING OFFICER'S RESPONSIBILITY

Commanding officers shall be responsible for:

A. Ensuring that all software used is legally acquired and installed.

B. Ensuring that access to sensitive data is limited to Department members on a need–to–know and right–to–know basis.

C. Ensuring that user manuals are accessible to members using computers.

D. Ensuring that computer use at the work location is monitored and is in compliance with Department guidelines.

680.30 ELECTRONIC COMMUNICATION - RIGHT TO PRIVACY

The content of all electronic communication, including but not limited to electronic mail (e-mail), e-mail attachments, instant messaging, text messaging, voice over internet protocol (VOIP), Twitter, Facebook and other 'electronic social media,' YouTube, records of internet use (including web sites accessed) and all other means of electronic communication (hereinafter "electronic communication") sent, received, or accessed through the Department's computer network, CAD system (by MDC or other terminal), Department cellular telephones, and other electronic communication devices provided by the Department are considered the property of the Department. This includes all electronic communication sent, received, or accessed from personal accounts (e.g. Yahoo, g-mail, etc.) on Department equipment.

As such, the Information Technology Division has the right to monitor, review, audit, and otherwise access the content of all electronic communication sent, received, or accessed on Department equipment with or without prior notice to the member for both non-investigatory work-related reasons, and for investigation of member misconduct. Members have no expectation of privacy or confidentiality in electronic communication sent, received, or accessed on Department equipment.
Electronic communication is subject to state record retention requirements and may be subject to the Wisconsin Public Records Law. The content of employee electronic communication may be subject to disclosure in litigation, audits, and other purposes. Users are authorized limited incidental use of the Department's resources for personal purposes, but members have no expectation of privacy or confidentiality in such use. Members are strongly encouraged to use their own communication devices for personal and confidential communications.

Members are prohibited from sending, receiving, or accessing electronic communication that is insulting, profane, vulgar, lewd, indecent, sexually explicit, illegal, profit-making, political, unprofessional, or in violation of the Department's policies, including but not limited to its EEO policies.

Edward A. Flynn

EDWARD A. FLYNN
CHIEF OF POLICE

EAF:djw